SECRET
Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9

D R A F T

DRAFT

MINIMUM SAFEGUARDS FOR PROTECTION OF "CRITICAL SYSTEMS" PROCESSING INTELLIGENCE INFORMATION

17 October 1983

by
DDCI COMPUSEC
SAFEGUARDS Working Group

25X1

SECRET
Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9

Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

DDCI Tasking; Approach for Developing Minimum SAFEGUARDS for "Critical Systems"; Selection of "Critical Systems"; Purpose of Field Coordination and Cost Assessments

II. OBJECTIVE AND GUIDELINES 4

Statement of Objective and Policy Guidelines; SAFEGUARDS Provided by Automated Systems Versus Environmental and Administrative SAFEGUARDS

III. MINIMUM SAFEGUARDS TO BE PROVIDED BY THE AUTOMATED SYSTEMS 7

Overview of DOD Trusted Computer System Evaluation Criteria; Overview of SAFEGUARDS to be Provided by the Automated "Critical Systems"; Strategy for Implementation of "Critical System" SAFEGUARDS:

- SAFEGUARD 1: Mandatory Access Control 12
- SAFEGUARD 2: Discretionary Access Control 14
- SAFEGUARD 3: Object Reuse 14
- SAFEGUARD 4: Labels 15
- SAFEGUARD 5: Label Integrity. 15
- SAFEGUARD 6: Exportation of Labeled Information 16
- SAFEGUARD 7: Exportation to Multilevel Devices. 16
- SAFEGUARD 8: Exportation to Single-Level Devices. 16
- SAFEGUARD 9: Labeling Human-Readable Output 17
- SAFEGUARD 10: Subject Sensitivity Labels 17
- SAFEGUARD 11: Device Labels. 18
- SAFEGUARD 12: Identification and Authentication. 18
- SAFEGUARD 13: Trusted Path 19
- SAFEGUARD 14: Audit. 19
- SAFEGUARD 15: System Architecture. 20
- SAFEGUARD 16: System Integrity 21
- SAFEGUARD 17: Covert Channel Analysis. 21
- SAFEGUARD 18: Trusted Facility Management. 21
- SAFEGUARD 19: Security Testing 21
- SAFEGUARD 20: Design Specification and Verification. 22
- SAFEGUARD 21: Configuration Management 22

Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9

Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9

TABLE OF CONTENTS
(Continued)

Page

IV. MINIMUM SECURITY SAFEGUARDS TO BE PROVIDED BY ENVIRONMENTAL AND ADMINISTRATIVE CONTROLS. 24

Administrative SAFEGUARDS

- SAFEGUARD 22: System Security Plan 25
- SAFEGUARD 23: External Marking of Removable Storage Media. . 25
- SAFEGUARD 24: Intelligent Terminals and Personal Computers . 25
- SAFEGUARD 25: Clearance of Maintenance Personnel 26
- SAFEGUARD 26: Annual Accreditation Requirement 26
- SAFEGUARD 27: Accreditation Authority for Automated Message Processing Systems 26
- SAFEGUARD 28: Accreditation of Automated Message Handling Systems. 27
- SAFEGUARD 29: Accreditation Recording. 27
- SAFEGUARD 30: Control Mechanisms in Automated Message Handling Systems 27
- SAFEGUARD 31: Automated Message Handling System Auditing Capabilities 28
- SAFEGUARD 32: Prohibition on Use of Unencrypted and Dial-up Lines. 28
- SAFEGUARD 33: Protection of Security-Related Software. . . . 28
- SAFEGUARD 34: Separation of Duties 28
- SAFEGUARD 35: Access Authorization Approvals 29
- SAFEGUARD 36: Awareness of and Compliance with Appropriate Security Policies. 29
- SAFEGUARD 37: Two Independent Access Authentication Mechanisms 29

Environmental Protection to be Afforded "Critical Automated Systems"

- SAFEGUARD 38: Physical Security. 30
- SAFEGUARD 39: Personnel Security 30
- SAFEGUARD 40: TEMPEST. 31
- SAFEGUARD 41: COMSEC 31

Declassified in Part - Sanitized Copy Approved for Release 2012/10/05 : CIA-RDP89B01354R000500640017-9